Task 3.1 Certification and Accreditation

Task Overview

FSA systems will undergo certification and accreditation for the first time during CY 03. BearingPoint will assist the Security and Privacy team review certification packages, recommend improvements to the certification packages, and coordinate the submission of test packages to the Department's Certification review group. Additionally, BearingPoint will assist FSA system's obtain access to EDCAS, answer content-related questions throughout the C&A process, and meet with FSA systems to prepare for C&A.

Task Details

FSA Certification and Accreditation will proceed along several paths:

- Preparation of the Xacta tool
- Direct support to system C&A teams to prepare for C&A
- Post C&A support to address remediations and POA&Ms

The process of tailoring the Xacta tool already was completed in June. We began our work by reviewing the extent OCIO has tailored the tool and what areas remain. Our team reviewed 453 C&A security requirements and associated test procedures. We added test procedures to most of the security requirements, reworded those requirements that were unclear, and deleted duplicates requirements. OCIO reviewed our work and stated they concurred with our updates. OCIO then delivered our joint comments to Xacta who completed updating the tool on June 18, 2003.

<u>Direct support to system C&A teams to prepare for C&A</u>
C&A is a new process within FSA and the Department. FSA system personnel will need frequent guidance and support throughout the C&A process. The security and privacy team will need to respond to these requests in a coordinated and consistent manner.

We now have roles and responsibilities identified for all FSA systems. We have conducted C&A kickoff meetings with most FSA systems, exploring system boundaries and identifying next steps.

A portion of the assistance we provided FSA system personnel is in the area of system boundary definitions. Although a constant challenge within FSA and the systems community, system boundaries are critical to the C&A process. We provided each C&A team a system boundary worksheet and system component worksheet to assist them consistently documented their system.

C&A requires the completion of several security-related documents. We have offered and provided our assistance in reviewing and commenting on C&A documentation. Where possible, we have provided tools and checklists to the C&A teams to first review their documents for compliance themselves prior to submission to the C&A team.

During the uploading of information into the Xacta tool, C&A teams certainly had many questions and issues that needed rapid resolution. The security and privacy team offered immediate "help desk" assistance to anyone requesting Xacta assistance. Our team either answer the questions or requested assistance from the company hosting Xacta or Xacta itself.

The security and privacy team interacted with all FSA systems throughout the C&A process. We devoted extra attention on the three CIO systems. We periodically met with the VDC, NSLDS,

and SAIG personnel to observe their C&A status. Where necessary, our team will shift resources to assist these personnel complete their C&A objectives.

To prepare EDCAS data entry personnel for use of the tool, we assisted FSA arrange for training on the tool. Once trained, we worked with FSA Personnel Security to verify the clearances of each person accessing the system. BearingPoint then worked with FSA to generate user IDs and passwords for only those employees and contractors trained in the tool. We created instructions for system use, worked with OCIO to finalize an EDCAS Rules of Behavior, and distributed User ID and passwords to those systems going through C&A this CY.

The majority of our support for the July/August period centered around direct support to FSA's systems. We met frequently with systems to discuss EDCAS data entry issues, and we spent a significant amount of time working on ST&E plans. As a group, BearingPoint and FSA system representatives determined which C&A requirements were not applicable. Each system began with roughly 450 requirements that needed to be reviewed one-by-one and then updated in the tool. The experience was valuable for the SSOs and their contractors for many reasons. Primarily, the CRG will not waste time asking systems questions that do not apply to their system. This process will go much smoother because of these pre-planning efforts.

During the September/October 2003 period, our support focused on assisting FSA systems work with the CRG. The CRG conducted kickoff interviews and executed ST&E plans on many FSA systems. We attended each of the meetings and supported our systems to ensure a smooth transition into the Certification process. Many SSOs and contractors requested support during the CRG's execution of the ST&E plans. We assisted FSA personnel respond to inquiries, clarify the CRG's intent, and draft responses to the CRG. Several FSA systems have successfully achieved full certification and accreditation in part due to the assistance of BearingPoint's FSA security team.

During the November/December time period, we assisted FSA's C&A teams through their system owner outbriefs and remediation activities. We supported over 15 outbriefs with the ED/CIO CRG and the C&A teams. During the outbriefs we assisted the teams understand the results of the C&A testing and provided a roadmap for success. Due in part to our support, all FSA systems were recommended for full certification and accreditation.

We now have begun assisting the Group 3 systems through the C&A process. This work includes meetings with SSOs, assisting C&A teams complete the required security documents, and reviewing completed documents before submission to the CRG. We also assisted C&A teams understand and remediate findings during the pre-certification review.

We continue to support CSB through its C&A hurdles. Our greatest challenge has been to teach the hired contractor how to complete security documentation and a C&A timeline. Even though this seems peculiar, our team has supported the CSB SSO in whatever capacity necessary. We support her decisions and offer counsel to remediate problems.

<u>Post C&A support to address remediations and POA&Ms</u>

Every FSA system will have numerous corrective actions after the certification group tests its system. The security and privacy team will assist each system create reasonable remediation plans and format these remediations into the POA&M format. We will assist system personnel address cost considerations, the benefits or drawbacks of certain mitigation strategies, and create realistic timelines to implement corrective actions.

Task Status

All requirements of this task are complete.